key : 1110000111

key 1 : 1 0 1 0 0 1 1 1 0
1 2 3 4 5 6 7 8

key 2 : 1 1 0 0 1 1 1 1

IP, EP, K1, K2, So, SW, P4, IP

10-bit key

1 2 3 4 5 6 7 8 9 10
1 1 1 0 0 0 0 1 1 1

P10: 3 - 5 - 2 - 7 - 4 - 10 - 1 - 9 - 8 - 6
1 0 1 0 0 0 1 1 1 0

Left

1 0 1 0 0

shift by 1 bit

0 1 0 0 1

Right

1 1 1 0

shift by 1 bit

1 1 1 0 1

merge

1 2 3 4 5 6 7 8 9 10
0 1 0 0 1 1 1 1 0 1

P8: 6 3 7 4 8 5 10 9

1 0 1 0 1 1 1 0

0 1 0 0 1 | 1 1 0 1

0 1 0 0 1 1 1 1 0 1

Left

Right

merge:

1 2 3 4 5 6 7 8 9 2x

0 1 0 0 1.

Ls-2

1 1 1 0 1

Ls-2

1 0 1 1 1

00101

merge

1 2 3 4 5 6 7 8 9 x

00101 10111

P8:

6-3-7-4-8-5-x-9

1 1 0 0 1 1 1 key2

8 bit plaintext

1 2 3 4 5 6 7 8

1 0 0 0 0 0 0 1

IP: 2-6-3-1-4-8-5-7.

0 0 0 1 0 1 0 0

Left 4 bits

0 0 0 1

right 4-bits

0 1 0 0

Right 4-bits

1 2 3 4

0 1 0 0

E/p: 4 1 2 3 2 3 4 1

0 0 1 0 1 0 0 1

XOR: 0 0 1 0 1 0 0 1

⊕

1 0 1 0 1 1 1 0 (key 1)

1 0 0 0 0 1 1 1

Left 4 bits:

First & last

1 0 0 0 : 1, 0 = 1

second & third: 0, 0 = 0

row 1 col 0 = 0

0 0

in bits: 0-0

Right 4 bits

0 1 1 1

First & last

0, 1 = 2

second and third

1 1 = 3

row 2, col 3

0 0

in bit

0-0

new 4 bit

1 2 3 4

0 0 0 0

p4: 2 4 3 1

0 0 0 0

1010

Left 4 bit

4

Subject :

XOR:

1 0 1 0
0 0 0 0
1 0 1 0

right
1 1 1 0

switch

Left 4 bits
1110

Right 4 bit
1 0 1 0

Right bits
1 - 2 - 3 - 4
1 0 1 0

I/P:
4 1 2 3 2 3 4 1
0 1 0 1 0 1 0 1

xor:
0 1 0 1 0 1 0 1
⊕ 1 1 0 0 1 1 1 1 (key 2)
1 0 0 1 1 0 1 0

Left 4 bits
1 0 0 1

first & last = 11 = 3
second & Third = 00 = 0

Right 4 bits
1 0 1 0
First & last = 10
1
second & third
$1 0^{0} = 1$

Subject :

4 5

row 3 = 2 → 01
col 0

inbit = 01

row 1 =
col 1 = 0

0 0
inbit: 0 0

New 4 bit
1 2 3 4
0 1 0 0

Left
1110

2 4 3 1
1 0 0 0

1 1 1 0
XOR 1 0 0 0
0 1 1 0

(Left 4 bits)

Right
1010

1 2 3 4 5 6 7 8
0 1 1 0 1 0 1 0

IP⁻¹: 4 1 3 5 7 2 8 6
0 0 1 1 1 1 0 0

This is 8-bit cipher text